UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/602,854	06/25/2003	Louis A. Stilp	RFID-0107	2099

23122 7590 04/06/2005

RATNERPRESTIA
P O BOX 980
VALLEY FORGE, PA 19482-0980

EXAMINER	
STONE, JENNIFER A	

ART UNIT	PAPER NUMBER
2636	

DATE MAILED: 04/06/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/602,854	STILP, LOUIS A.	
	Examiner	Art Unit	
	Jennifer A Stone	2636	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 January 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-3 and 5-42* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3 and 5-42* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *25 June 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *11/1/2004*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

Claim Rejections - 35 USC § 112

1. The claim rejections are withdrawn based on the amended claim language.

Claim Rejections - 35 USC § 103

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 103 that form the basis for the rejections under this section made in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claim 1-3, 23, 29-34, 36-38, and 42 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ciarcia, JR et al. (US 2004/0189471).

For claim 1, Ciarcia discloses a first RFID reader (parag 0026, lns 3 and 4) for use in a security network in a building having a sensor (parag 0047, lns 23-27; Fig. 1, item 104), an RFID transponder coupled to the sensor for wirelessly transmitting a signal indicating a status of the sensor (paragraph 0020, lns 9-12; parag 0021; lns 1-10; parag 0027, lns 1-4; parag 0055, lns 1, 2, and 9-18), the first RFID reader comprising: wirelessly communicating with the RFID transponder (parag 0023, lns 1-5; parag 0026, lns 1-4); and a processor configured to receive the wireless signal (parag 0030, lns 1-7; Fig. 4, item 240), decode the sensor status from the wireless signal, and communicate the sensor

status to a first control function (parag 0024, lns 4-16; parag 0028, lns 10-19). Even though Ciarcia does not disclose an antenna, it would have been extremely obvious to one of ordinary skill in the art, at the time the invention was made to include an antenna coupled to the processor for wirelessly communicating with the RFID transponder to enhance signal propagation.

For claim 2, the security network is configured for use in a building having an opening and the sensor monitors the opening to detect intrusion (parag 0027; Fig. 2, item 204).

For claim 3, Ciarcia discloses the security network configured for use in a building and the sensor monitors the building for smoke or fire (parag 0048, last 6 lines; Fig. 2, item 216).

For claim 23, Ciarcia discloses the first RFID reader to comprise a sensor that monitors an environmental parameter in at least one portion of the building (parag 0048, last 6 lines).

For claim 29, an operation of the first RFID reader is under the control of the master controller contained within the security network (parag 0028, lns 14-24). The monitoring station functions as the master controller controlling conditions of security equipment such as door locks.

For claim 30, the master controller is contained within a device in the security network other than the first RFID reader (parag 0046, lns 1-10; parag 0047, lns 1-10; Fig. 2, item 212; Fig. 6, item 400).

For claim 31, Ciarcia discloses the first RFID reader (parag 0030, lns 1-12; parag 0035, lns 1-5) comprising a master controller. The first reader comprises

the devices of the adaptive console. The display and keyboard console is considered a master controller because an individual can control system functions using the console.

For claim 32, the master controller sends a command controlling at least one operation of another device (Fig. 3, items 12, 24, and 26) within the security network (parag 0028, lns 14-21).

For claim 33, Ciarcia discloses the first RFID reader comprising configuration data that is changed under the control of the master controller or control function contained within the security network (parag 0041, last 4 lines; parag 0047, lns 6, 7, and 19-23).

For claim 34, Ciarcia discloses the first reader comprising a memory, which stores program code executed by the processor wherein the program code is updatable under the control of the master controller or control function contained within the security network (Fig. 4, items 250 and 260; parag 0033, 23-31; parag 0034; parag 0038, lns 27-30).

For claims 36, the first RFID reader comprises an interface to another security system (parag 0047, lns 1-10 and 25-29; parag 0048, lns 1-4; Fig. 2, items 212).

For claim 37, Ciarcia does not disclose the first RFID reader to receive power via the interface to the other security system. However, it would have been obvious to provide a single source of power among a plurality of readers for multiple security systems to ensure operability of all the readers. Without power the system will not function.

For claim 38, Ciarcia discloses the first RFID reader to transmit commands via the interface to the other security system (Fig. 2, item 212); however, it would have been obvious to provide commands to the first RFID reader via the bidirectional communication path, as disclosed by Ciarcia (see bidirectional communication between items 212 and 106, Fig. 2) so that the first reader is informed of the status of the other security system.

For claim 42, the control function is performed by the first RFID reader (parag 0028, lns 14-17).

4. Claims 5-9, 11, 13-15, 18, 19, and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ciarcia, JR et al. (US 2004/0189471) as applied to claim 1 above, and further in view of Pratt (US 2004/0066280).

For claim 5, Ciarcia discloses the security network to include a second reader (Fig. 2, item 212), and the first RFID reader (Fig. 2, item 106) receives communication from the second reader (see bidirectional arrow between items 212 and 106). However, it is unclear if the second reader is an RFID reader or if the reader transmits an RFID signal. Pratt, however, discloses first and second RFID readers that communicate bidirectional RFID signals (parag 0018; parag 0019, lns 1-11). It would have been obvious to use a second RFID reader that communicates to a first RFID reader to establish a consistent means of communication (RF) throughout a system. In addition, an RF system eliminates ergonomical hazards associated with wiring.

For claim 6, the security network includes a second reader (Fig. 2, item 212) and the first RFID reader transmits wireless communications received from

the RFID transponder (Fig. 2, items 202, 224, 206, 204, and 208) to the second reader (Fig. 2, item 212). It would have been obvious to communicate RFID signals from the first RFID reader to a second RFID reader to establish a consistent means of communication (RF) throughout a system. In addition, an RF system eliminates ergonomical hazards associated with wiring.

For claim 7, Ciarcia does not disclose a second antenna with the first RFID reader; however, Pratt discloses using more than one antenna with a reader (parag 0027; Fig. 2 items 14 and 30). It would have been obvious to incorporate more than one antenna on the RFID reader to facilitate various modes of communication.

For claim 8, Ciarcia does not disclose a second antenna with the first RFID reader; however, Pratt discloses the first RFID reader to use only one of the first antenna or the second antenna in each wireless communications (parag. 0027). It would have been obvious to incorporate the second antenna for use in passive applications.

For claim 9, Ciarcia does not disclose determining antenna configuration. Pratt, on the other hand, uses configuration data that determines which of the first antenna or the second antenna to use in each wireless communications (parag 0029, lns 1-3; parag 0030; parag 0058, lns 7-12). It would have been obvious to use configuration data so the reader automatically determines the type of antenna appropriate for communication.

For claim 11, Ciarcia does not disclose supporting more than one modulation technique; however, Pratt discloses the RFID reader to support more

than one modulation technique (parag 0012, lns 1-6; parag 0035, lns 3-6; parag 0037, lns 1-7). It would have been obvious to provide the RFID reader to support more than one modulation technique in order to conserve electrical energy (parag 0036, lns 12-16).

For claim 13, Ciarcia does not disclose the first RFID to include Gaussian Frequency Shift Keying; however, Pratt discloses this feature (parag 0031). It would have been obvious to use Gaussian Frequency Shift Keying so that more than one modulation technique is used for further enhancing the security of the system.

For claim 14, Ciarcia does not disclose supporting more than one transmission power level; however, Pratt discloses the RFID reader to support more than one transmission power level (parag 0025, lns 1-8). It would have been obvious to provide the RFID reader to support more than one transmission power level in order to conserve electrical energy (parag 0036, lns 12-16).

For claim 15, Ciarcia does not disclose the reader to vary its rate of transmitting RF energy; however, Pratt discloses the RFID reader to vary its rate of transmitting RF energy (parag 0037, lns 1-7). It would have been obvious to provide the RFID reader to support more than one rate of RF transmission order to conserve electrical energy (parag 0036, lns 12-16).

For claim 18, Ciarcia does not disclose the first reader to include an acoustic transducer. Pratt, on the other hand, does disclose a detector that transmits an acoustic signal to a reader (parag. 0019, lns 12-17). It would have been obvious to wirelessly communicate acoustic signals to detect sound.

For claim 19, Ciarcia does not disclose the RFID reader to process audio waves. Pratt, on the other hand, does disclose a detector that transmits an audio or acoustic signals to a reader (parag. 0019, lns 12-17). It would have been obvious to include an acoustic signal to detect sound as well as glass breakage.

5. Claim 10 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ciarcia, JR et al. (US 2004/0189471) as applied to claim 1 above, and further in view of Brooking (U.S. 2002/0070863).

Ciarcia does not disclose a battery backup with the first RFID reader, however, it is clear that Brooking provides an RFID reader that contains a backup battery (parag 0042, lns 1-4 and 12-15; Fig. 3, item 33). It would have been obvious to include a backup power source to support a primary power source in the event of a power failure of the primary power source.

6. Claim 12 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ciarcia and Pratt, and further in view of Durtler (U.S. 6,271,754).

Ciarcia does not disclose continuous wave modulation; however, Durtler discloses continuous wave modulation between a transmitter and receiver (col 2, lns 16-19). It would have been obvious to provide a reader or receiver that supports continuous wave modulation frequency in order to accurately detect motion from an intruder.

7. Claim 16 and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ciarcia, as applied to claim 1, and further in view of Zaharia (U.S. 6,707,374).

For claim 16, Ciarcia discloses an RFID reader to contain an algorithm for processing environmental parameters in a security application (parag 0039); however, the use of Doppler analysis is not used. However, Zaharia discloses motion detectors along with RFID sensors/readers that use Doppler microwave analysis. The Zaharia reference also pertains to a security application (col 2, lns 16-23 and 38-40; Fig. 2, item 25). It would have been obvious to use Doppler motion detectors incorporated in RFID readers in order to quantify a number of persons/objects in a secure area in order to enhance security.

For claim 17, Ciarcia discloses an RFID reader to contain an algorithm for processing environmental parameters in a security application; however, the use of Doppler analysis is not used. However, Zaharia discloses motion detectors to detect motion to the response wireless communications from a first RFID transponder (col 1, lns 34-48). The transponders are the RFIDs associated with each individual to provide wireless communication to and from the motion detector. It would have been obvious to use Doppler motion detectors incorporated in RFID readers in order to quantify a number of persons/objects in a secure area in order to enhance security.

8. Claims 20-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ciarcia and Pratt, as applied to claim 18, and further in view of Moskowitz et al. (U.S. 6,483,433).

For claim 20, Pratt does not disclose performing voice recognition. Moskowitz discloses a security access control system that uses an audio detector to perform voice recognition (col 2, lns 37-40; col 3, lns 16-19, 26, and

27; col 4, lns 38-47 and 62-67). It would have been obvious that the RFID readers of both Pratt and Ciarcia incorporate voice recognition, in an access control environment, in order for an individual to leave a message at an entrance point with the intention of being delivered to a recipient.

For claim 21, Ciarcia discloses a processor configured to perform the control function in response to sensor commands (parag 0028, lns 14-22); however, the commands are not received via voice recognition. Moskowitz discloses a reader to accept voice recognition (Fig. 2, items 270, 250, and 260; col 4, lns 38-47 and 62-67). It would have been obvious that Ciarcia accepts voice recognition, in an access control environment, in order for an individual to leave a message at an entrance point with the intention of being delivered to a recipient.

For claim 22, Ciarcia discloses the RFID reader further to contain algorithms to process frequency waves received by sensors and Pratt discloses the acoustic transducer; however neither Ciarcia nor Pratt disclose retransmitting digitized audio waves via wireless communications. Moskowitz discloses this feature (col 3, lns 5-15; Fig. 3, items 300 and 320; Fig. 2, item 220; col 4, lns 56-67; col 5, lns 40-44). It would have been obvious that Ciarcia accepts and retransmits audio data, in an access control environment, in order for an individual to leave a message at an entrance point with the intention of being delivered to a recipient in a wireless manner.

9. Claims 24-26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ciarcia and further in view of Skinner (U.S. 6,703,930).

For claim 24, Ciarcia discloses RFID readers to receive environmental parameters, such as fire. Skinner, on the other hand, discloses RFID readers to receive data regarding the presence of smoke (col 4, lns 10-15, 54, and 55). It would have been obvious to detect smoke in order to notify an individual of a potential fire in a residential environment.

For claim 25, Ciarcia discloses RFID readers to receive environmental parameters, but does not disclose temperature. Skinner, on the other hand, discloses RFID readers to receive temperature data (col 3, lns 15-19; col 4, lns 13-16, 31-32, and 54-57). It would have been obvious to detect an extreme temperature so that climate control can be implemented on the system thereby promoting energy efficiency.

For claim 26, Ciarcia discloses RFID readers to receive environmental parameters, but does not disclose water detectors. Skinner, on the other hand, discloses RFID readers to receive notification of the presence of water (col 3, lns 15-19; col 4, lns 13-16, 31-32, and 54-57). It would have been obvious to detect the presence of water in order to notify an individual of excessive water levels in a residential environment.

10. Claims 27 and 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ciarcia and further in view of Moskowitz et al. (U.S. 6,483,433).

For claim 27, Ciarcia does not disclose a camera in the RFID reader; however, Moskowitz does disclose a camera in combination with an RFID reader (col 4, lns 42-47 and 56). It would be obvious to disclose a camera in

combination with an RFID reader in order to enhance the security of the access control system. Not only data, but a photograph plus data can be transmitted to a recipient.

For claim 28, Ciarcia discloses the RFID reader to contain algorithms (col 6, lns 25 and 26) to process frequency waves received by the environmental parameters, but does not disclose a camera for wireless transmission. Moskowitz does disclose a reader to digitize pictures recorded by the camera, and transmit the digitized pictures via wireless communications (col 6, lns 21-26, 30-35, and 49-52). It would be obvious to disclose a camera for transmitting photos to a recipient in order to enhance the security of the access control system.

11. Claims 39-41 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ciarcia and further in view of Lancaster (U.S. 2003/0227385)

For claim 39, Ciarcia does not disclose mounting structure specifics of the first RFID reader; however, Lancaster discloses an RFID reader that is mechanically mounted to a plate, wherein the plate is configured to be mechanically mounted to an outlet (parag 0012, lns 1-4). It is well known that an electrical box contains an electrical outlet. It would be obvious to mount an RFID reader to a plate, such as an electrical box in order to identify the electrical box. Identification is a key factor in terms of security.

For claim 40, Ciarcia does not disclose mounting structure specifics of the first RFID reader; however, Lancaster discloses an RFID reader integrated with an outlet, and configured to be installed within a standard outlet box approved for

use within buildings (parag 0016, lns 7-9; Fig. 8 – Electrical Box, RFID/EAS tag). It would be obvious to mount an RFID reader to a plate, such as an electrical box or power outlet in order to identify electrical devices. Identification is a key factor in terms of security.

For claim 41, Ciarcia does not disclose mounting structure specifics of the first RFID reader; however, Lancaster discloses an RFID reader that is integrated with an electrical box, and configured to be installed within a standard outlet box (parag 0016, lns 7-9; Fig. 8 – Electrical Box, RFID/EAS tag). It is well known that light switches can be installed in standard outlet boxes. It would be obvious to mount an RFID reader to a light switch in order to identify the switch. Identification is a key factor in terms of security.

12. Claim 35 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ciarcia as applied to claim 1 above, and further in view of Berquist et al. (US 2001/0008390).

Ciarcia does not disclose the RFID transponder within the packaging of the RFID reader; however, Berquist discloses this feature (parag 0014, lns 1-5; Fig. 1). It would be obvious to enclose the transponder within the physical packaging of the reader to protect the transponder from environmental elements.

Response to Amendment/Argument

13. Applicant's arguments with respect to claims 1-3, and 5-42 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

14. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Jennifer Stone
March 25, 2005

JEFFERY HOFSASS
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2600